UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The SUBJECT OFFICE at 7605 North San Fernando Road, Burbank, California 91505	)	Case No. 2-18-MJ-01713

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30).*

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

_____
Judge's signature

City and state: Los Angeles, California

Hon. Alicia G. Rosenberg
Printed name and title

AUSA: Alex Wyman (x2435)

Return		
Case No.: 2-18-MJ-01713	*Date and time warrant executed:*	*Copy of warrant and inventory left with:*

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The subject premises is an office (the "SUBJECT OFFICE") associated with Printograph, Inc., doing business as GotPrint.com ("Printograph"), located within 7605 North San Fernando Road in Burbank, California, 91505. It is a large, two-story office building with the number 7605 on the exterior near the entrance. There is a large sign on the exterior of the building with the name GotPrint.com in white letters and a black background. The exterior of the building is white and beige with large exterior windows. The SUBJECT OFFICE is located on the first floor of this building against the exterior windows facing towards North San Fernando Road. The SUBJECT OFFICE is the third door on the right from the interior entrance to the Printograph offices from the building's main lobby. There is no office number on the SUBJECT OFFICE. The SUBJECT OFFICE is rectangular with yellow and brown walls and with large rectangular windows facing inwards that provide a full view of the interior from the hallway. Inside the SUBJECT OFFICE, there is a desk with a computer, multiple monitors, and papers and binders on it. There are multiple filing cabinets against opposing walls. There are boxes on the floor. There is also a table and chairs.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The following items are to be seized from the SUBJECT OFFICE, which constitute fruits, evidence, and instrumentalities of criminal violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (wire fraud), and 1957 (money laundering) (collectively, the "SUBJECT OFFENSES"):

a. Any and all documents and records relating to any financial or bank accounts owned or controlled in whole or in part by SHODJA TALAEE, also known as Sean Edin Talaee ("TALAEE"), from December 2014 to the present.

b. Any and all documents relating to any financial transactions conducted or caused to be conducted by TALAEE or companies affiliated with TALAEE, from December 2014 to the present.

c. Any and all accounting, auditing, or tax documents or records relating to any business or other financial activities of TALAEE, from December 2014 to the present.

d. Any documents reflecting or relating to the incorporation of, ownership of, or licensing for any business ventures or activities of TALAEE, from December 2014 to the present.

e. Any and all documents, records, or communications with the Internal Revenue Service, from December 2014 to the present.

f. Any and all documents, records, or communications related to or with actual or potential investors, clients, or

customers of, or lenders to, any business activities or ventures related to TALAEE, from December 2014 to the present.

g. Any and all memoranda of understanding, business contacts, or business agreements, including any debt instruments, entered into by TALAEE or any entity affiliated or associated with TALAEE.

h. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

i. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output

devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine

whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized,

the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the SUBJECT OFFENSES;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, John Verrastro, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a warrant to search an office associated with the closely held corporation Printograph, Inc., doing business as GotPrint.com ("Printograph"), located at 7605 North San Fernando Road in Burbank, California, 91050 (the "SUBJECT OFFICE"), and as described fully in Attachment A, which is incorporated herein by reference. The SUBJECT OFFICE was previously occupied by a former employee known to Printograph as SHODJA TALAEE, also known as Sean Edin Talaee ("TALAEE"), until Printograph terminated TALAEE's employment on or about June 20, 2018. The SUBJECT OFFICE contains both personal items belonging to TALAEE and business items belonging to Printograph.

2. As described more fully below, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of criminal violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (wire fraud), and 1957 (money laundering) (collectively, the "SUBJECT OFFENSES"), as described more fully in Attachment B, will be found in the SUBJECT OFFICE.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, my review of reports drafted by other employees, and information obtained from various law enforcement personnel and witnesses. This

affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND FOR SPECIAL AGENT JOHN VERRASTRO

4. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI"), United States Department of Justice, in the Los Angeles Field Office and have been so employed since 2004. For the past approximately twelve years, my primary responsibility has been investigating securities fraud, mail fraud, wire fraud, money laundering, and other fraud violations. My experience includes interviewing witnesses, gathering documents, analyzing financial documents, conducting surveillance, and serving grand jury subpoenas. I have also received training in investigating financial crimes, including securities fraud, bank fraud, wire fraud, and money laundering. Prior to becoming an FBI agent, I worked for ten years in financial services at a bank and an investment firm. In the course of my FBI employment, I have participated in executing many search warrants of businesses and residences in connection with financial fraud offenses.

5. In investigating fraudulent schemes, I have become familiar with the types of records and documents that individuals and entities use to perpetrate their schemes, and have executed and participated in the execution of search

warrants at homes and businesses of individuals involved in fraudulent schemes.

III. SUMMARY OF PROBABLE CAUSE

6. Between 2014 and 2018, Printograph employed TALAEE as its Controller of Accounting. TALAEE had access to Printograph's accounting records and could review Printograph's bank account information and activity. Beginning in 2015, TALAEE periodically paid Printograph's "estimated tax" throughout the year rather than paying Printograph's taxes all at once at the end of the year. TALAEE would prepare a check made payable to the United States Treasury and present it to Printograph's president, Sonik Artounian ("Artounian"), for Artounian to sign. TALAEE would then submit the check to the Internal Revenue Service ("IRS") along with a voucher form requesting that the IRS credit Printograph with the tax payment. On many occasions, however, TALAEE provided his own personal information, including his last name and Social Security Number ("SSN"), in filling out the voucher form, thereby claiming the tax payments for himself, rather than on behalf of Printograph.

7. While he was employed by Printograph, TALAEE worked in the SUBJECT OFFICE. Many of TALAEE's business records, accounting records, and financial documents, as well as unopened mail addressed to TALAEE, remain in the SUBJECT OFFICE.

IV. STATEMENT OF PROBABLE CAUSE

8. Based on conversations with witnesses, victims, and other FBI SAs and my knowledge of the investigation, I know the following:

a. Artounian hired TALAEE near the end of 2014 as the Controller of Accounting for Printograph. In this position, TALAEE had access to Printograph's accounting records and could review Printograph's bank account information and activity, although TALAEE lacked signing authority or wire transfer authority for these accounts.

b. At the time TALAEE was hired, Printograph maintained a bank account in which it would save money to pay the IRS its tax liability at the end of the year. TALAEE recommended to Artounian that Printograph pay installments of its "estimated tax" throughout the year rather than paying its actual tax liability all at once at the end of the year. Artounian agreed, and in 2015 Printograph began a practice of providing periodic payments to the IRS for its "estimated tax" throughout the year. As part of this practice, TALAEE would periodically bring checks to Artounian, who had signing authority for Printograph's bank accounts, to sign so that TALAEE could submit them to the IRS. TALAEE would then fill out a voucher form requesting that the IRS credit Printograph with the payments and then mail the check and the voucher form to the IRS. Artounian's understanding was that TALAEE would use Artounian's last name and SSN in filling out this form so that the vouchers they received would credit Printograph with the tax payments. This practice continued until 2018.

c. In February 2018, Artounian received a letter at her home address from the IRS requesting Artounian's assistance in a pending federal tax matter related to TALAEE. In response

to this letter, Artounian contacted IRS Revenue Agent Melissa A. Clark, whose contact information was included in the letter, and Artounian eventually met with Agent Clark in person. During this meeting, Artounian was provided with limited information about the tax matter involving TALAEE.

d. In June 2018, Artounian received another letter from the IRS. On or about June 20, 2018, Artounian met with Revenue Agent Clark again, as well as Revenue Agent Bernard Trapp, who provided Artounian with further information about the IRS's investigation into TALAEE. Through her conversations with the IRS, Artounian was able to determine that TALAEE was depositing the checks that Artounian had signed but that TALAEE appeared to be claiming some of the tax benefits for himself.

e. Following her discussion with the IRS agents, Artounian accessed Printograph's bank accounts in order to review copies of the checks that TALAEE had deposited with the IRS on behalf of Printograph. Artounian observed that some of these checks listed the first four letters of Artounian's last name and Artounian's SSN on the back of the negotiated checks, but that the back of other checks listed the first four letters of TALAEE's last name and the SSN that Printograph had on file for TALAEE. The checks listing the first four letters of TALAEE's last name and his SSN totaled well over $2 million.

f. Artounian provided me with copies of checks made payable to the United States Treasury, Internal Revenue Service, that had been negotiated against Printograph. These checks confirm what Artounian told me. The back of some of the checks

listed what Artounian told me was her SSN and the first four letters of Artounian's last name, while others listed TALAEE's SSN as well as the first four letters of TALAEE's last name.

g. On or about June 20, 2018, a Printograph employee contacted Artounian and told Artounian that TALAEE was boxing up documents in the SUBJECT OFFICE. Artounian returned to Printograph's offices and called TALAEE into her office, at which point she terminated TALAEE's employment. TALAEE was not permitted to return to the SUBJECT OFFICE. TALAEE's phone, wallet, and other personal effects were given to him, and he was escorted from the premises.

h. Also on or about June 20, 2018, Artounian contacted the FBI's Public Access Line by telephone to report that Printograph had been the victim of a multimillion-dollar embezzlement committed by TALAEE.

i. Printograph employee Kristina Keshishyan ("Keshishyan") contacted the FBI by telephone on or about June 20, 2018 and provided TALAEE's SSN and other personal identifying information. Keshishyan contacted the FBI by telephone again on or about June 21, 2018 and advised that TALAEE had forged signatures and created fake documents during his employment at Printograph.

j. On June 28, 2018, I spoke with Artounian, Keshishyan, and Printograph's outside counsel, Eric Puritsky ("Puritsky"), by telephone. During this conversation, Puritsky informed me that he had received a letter from TALAEE's attorney

requesting to have TALAEE's property in the SUBJECT OFFICE returned to him.

k. On June 29, 2018, Artounian informed me that she and other Printograph employees had looked through the SUBJECT OFFICE and observed what appeared to be personal bank account information addressed to TALAEE under the name "Sean Talaee."

l. On June 29, 2018, I visited Printograph's offices. Artounian showed me the SUBJECT OFFICE, though I did not search the SUBJECT OFFICE. I took pictures of the SUBJECT OFFICE through the windows in the hall. Inside the SUBJECT OFFICE, I saw documents sitting on a desk and in boxes located on a table and on the floor. I saw filing cabinets against the wall in the SUBJECT OFFICE with what appeared to be unopened mail. Artounian showed me documents on the desk in the SUBJECT OFFICE that appeared to be financial in nature. I also saw envelopes addressed to TALAEE in a notebook on the desk, as well as sealed envelopes addressed from TALAEE to other parties stacked on a filing cabinet.

m. I showed Artounian a photograph from the California Department of Motor Vehicles records for "Sean Edin Talaee," and Artounian identified the man in the photograph as the person who worked in the SUBJECT OFFICE.

V. TRAINING AND EXPERIENCE ON FRAUD OFFENSES

9. Based on my training and experience, I know the following: Individuals engaged in fraudulent schemes often keep the records and documents they use to perpetrate their fraud at their homes and businesses, in their vehicles, and on their

computers and other digital devices. In the normal course of business, hard copies of accounting records are often maintained in the offices of those employees who are responsible for the business's accounting. Business records are often kept for a period of seven years.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

10. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one

device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500-gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[1] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed

[1] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently

used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

11. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

12. For all the reasons described above, there is probable cause to believe that evidence of violations of the SUBJECT OFFENSES, as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT OFFICE, as further described above and in Attachment A of this affidavit.

John Verrastro, Special Agent,
Federal Bureau of
Investigation

Subscribed to and sworn before me
this 2nd day of July, 2018.

HONORABLE ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE